



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/381,056	12/21/1999	PAUL MERTES	2345/86	3457
26646	7590	12/27/2005		
KENYON & KENYON ONE BROADWAY NEW YORK, NY 10004			EXAMINER FIELDS, COURTNEY D	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 12/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/381,056

Applicant(s)

MERTES ET AL.

Examiner

Courtney D. Fields

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 21 October 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 4-9 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 4-9 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 4-9 are pending.

#### ***Response to Arguments***

2. Applicant's arguments filed 21 October 2005 have been fully considered but they are not persuasive.

3. Referring to the rejection of claim 4, the Applicant argues that the prior art (Bathrick) does not identically disclose or suggest the features of causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair, unequivocally assigning the at least one encryption key pair to the user, causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair, after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair, and encrypting the new certificate using the public key part of the at least one encryption key pair.

The Examiner respectfully disagrees and asserts that Bathrick discloses the features of causing the certifying authority (equivalent to a trust center) to provide the entity (equivalent to the user) with a previously generated, personalized, and certified signature key pair as shown in Column 2, lines 19-40. The certifying authority

(equivalent to a trust center) provides the entity (equivalent to the user) with keying material (equivalent to components for producing at least one encryption key pair) and issues (equivalent to assigned) the user with a public key using the keying material (equivalent to components for producing at least one encryption key pair) which is provided by the certifying authority (equivalent to a trust center) as shown in Column 2, lines 41-52. Once the certifying authority (equivalent to a trust center) receives a request from the entity (equivalent to the user), the certifying authority (equivalent to a trust center) authenticates (equivalent to check) the identity via a second communications by using the public key which was previously issued to the entity (equivalent to the user) as shown in Column 2, lines 53-57. After receiving a successful authentication, the requesting entity (equivalent to the user), protects the public key and address to the certifying authority (equivalent to a trust center) by using the keying material (equivalent to components for producing at least one encryption key pair) which was issued by the certifying authority (equivalent to a trust center) in Column 2, lines 58-63. Therefore, once the identity is confirmed/verified by the certifying authority (equivalent to a trust center), a new certificate is issued to the entity (equivalent to the user) via the second secure communications and the public key which is issued assigned to the entity by the certifying authority (equivalent to a trust center) for public use by other entities (equivalent to other users). The new certificate is encrypted by the public key which is a part of generated signature key pair as shown in Column 2, lines 64-67, and Column 3, lines 1-2.

4. Therefore, the rejection of claims 4-9 are maintained in view of the reasons above and in view of the reasons below.

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 4-9 are rejected under 35 U.S.C. 102(b) as being anticipated by Bathrick et al. (U.S. Patent No. 5,825,300).

Referring to claim 4, Bathrick et al. discloses a certifying authority (trust center) providing the entity (each end system and user) with a generated and certified signature key pair in Column 2, lines 19-40. The end system and user (entity) receives the keying material (components for producing one encryption key pair) from the certifying authority (trust center) and then generates a public key and a private key pair and protects (marking) the public key using the keying material provided by the certifying authority (trust center). (See Column 2, lines 41-52) Once the certifying authority (trust center) receives the request from the entity (each end system and user), the certifying authority authenticates the identity via a second secure communications by requesting the public key and address of the entity (each end system and user) is sent to the certifying authority (trust center). (See Column 2, lines 53-57) After receiving authentication, the requesting entity (each end system and user) protects the public key

and address to the certifying authority (trust center) by using the keying material (components for producing one encryption key pair) provided by the certifying authority (trust center). (See Column 2, lines 58-63) .Once the identity is confirmed, the certifying authority (trust center) issues a new certificate to the entity (each end system and user) via the second secure communications and records the public key of the entity (each end system and user) at the certifying authority for public use by other entities (other end systems and users) within the certifying authority domain. (See Column 2, lines 64-67, Column 3, lines 1-2).

Referring to the rejection of claim 5, Bathrick et al. discloses a certifying authority (trust center) providing the user with components for producing at least one encryption key pair in Column 2, lines 32-40, producing at least one additional signature key pair in Column 2, lines 41-52, and the user marks a public part of the additional signature key pair using the secret key of the previously generated signature key pair in Column 2, lines 53-63.

Referring to the rejection of claim 6, Bathrick et al. discloses checking the correctness of an assignment regarding one of the public part of at least one encryption key pair and verifying the signature and the validity of a new certificate in the certifying authority (trust center) in Column 2, lines 64-67, Column 3, lines 1-2.

Referring to claim 7, Bathrick et al. discloses a certifying authority (trust center) providing the entity (each end system and user) with a generated and certified signature key pair in Column 2, lines 19-40. The end system and user (entity) receives the keying material (components for producing one encryption key pair) from the certifying

Art Unit: 2137

authority (trust center) and then generates a public key and a private key pair and protects (marking) the public key using the keying material provided by the certifying authority (trust center). (See Column 2, lines 41-52) Once the certifying authority (trust center) receives the request from the entity (each end system and user), the certifying authority authenticates the identity via a second secure communications by requesting the public key and address of the entity (each end system and user) is sent to the certifying authority (trust center). (See Column 2, lines 53-57) After receiving authentication, the requesting entity (each end system and user) protects the public key and address to the certifying authority (trust center) by using the keying material (components for producing one encryption key pair) provided by the certifying authority (trust center). (See Column 2, lines 58-63) Once the identity is confirmed, the certifying authority (trust center) issues a new certificate to the entity (each end system and user) via the second secure communications and records the public key of the entity (each end system and user) at the certifying authority for public use by other entities (other end systems and users) within the certifying authority domain. (See Column 2, lines 64-67, Column 3, lines 1-2). Checking the correctness of an assignment regarding one of the public part of at least one encryption key pair and verifying the signature and the validity of a new certificate in the certifying authority (trust center) in Column 2, lines 64-67, Column 3, lines 1-2.

Referring to the rejection of claims 8-9, Bathrick et al. discloses wherein the secret part of the encryption key pair is not revealed by the user in Column 1, lines 42-47, and Column 2, lines 19-25.

***Conclusion***

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*cd*

cdf

December 20, 2005

*Matthew B. Smithers*  
**MATTHEW SMITHERS**  
**PRIMARY EXAMINER**  
*Art Unit 2137*